Venue Smart Pty Ltd

Anti-Money Laundering and Combating the Financing of Terrorism Policy

(AML/CFT Policy)

Document History (Version Number)	Date Modified	Author	Summary of Changes
V1.0	22nd August 2023	Franchesco Vorster	Initial Draft

Approved by the Board on: XXXX 20223

Contents

1.0 Definition

Capitalised terms used in this document have the following meaning, unless the context otherwise requires:

Aggregator (Aggregation) means a payment aggregation service used to process BPay, Direct Entry and NPP transactions provided by a Service Provider to Venue Smart and on-supplied by Venue Smart to Merchants;

AML/CFT Act means the *Anti-Money Laundering and Countering Financing of Terrorism Act 2006* ;

AML/CFT Policy means the anti-money laundering and combating the financing of terrorism policy and processes developed by Venue Smart to detect ML and FT and manage and mitigate the risk of ML and FT;

AML/FT Risk Assessment means this document which records Venue Smart assessment of the risk of ML and FT as amended from time to time;

AML/CFT Risk Register means the register of risk maintained by the General Manager, Payments;

Beneficial Owner means any individual (natural person) who, satisfies any one (or any combination) of the following three elements:

- Has Effective Control of a Merchant;
- Has Effective Control of the person on whose behalf a transaction is conducted; or
- Who owns a prescribed threshold (being more than 25%) of the Merchant or person on whose behalf a transaction is conducted,

and "Beneficial Ownership" will have a similar meaning;

Note: It is possible for ownership to be split into parcels of 25 percent or less but, if the Merchant's ownership structure is understood at each layer, it might become apparent that relationships between the parties may give an individual aggregate ownership of the Merchant that amounts to more than 25 percent.

Board means the Venue Smart board of directors from time to time;

BPay means that payment type, supplied by the banks, that allows a payer to pay a biller using a BPay biller reference and a payer customer reference;

Card Acquirer means a business that has the right (allocated to them by a card Association/Scheme) to acquire card payments from a Merchant and send that payment to the Issuer of that card. The Acquirer either utilises insourced or outsourced technologies to

perform this function. The Card Acquirer also means Global Payments and Fiserv or such other replacement or successor appointed by Venue Smart from time to time;

Chargebacks means the dispute process that results in the return of money or the reversal of a card transaction initiated by the Card Acquirer or a Merchant's customer's issuing bank;

Complaint means an expression of dissatisfaction made to Venue Smart by any person, related to its products or services, or the complaints handling process itself, and dispute has a corresponding meaning;

Complaints Policy means complaints and disputes policy including any schedules to it as amended from time to time;

Complaints Register means the register of Complaints maintained by the General Manager, Payments.

Compliance Manager means the staff member appointed by Venue Smart to manage compliance;

Credit Management Team means the group of staff appointed by Venue Smart to manage credit risk;

Credit Risk Policy means this credit risk policy as amended from time to time;

Direct Entry means that payments type, inclusive of direct debits and direct credits, supplied by a Service Provider that allows a payee to debit a bank account and a payer to credit a bank account overnight.

Dispute means the dispute process that results in the return of money or the reversal of a Direct Debit, NPP or BPay transaction initiated by the Service Provider or a Merchant's customer's bank;

Effective Control means to:

- any individual(s) with the ability to control the Merchant and/or dismiss or appoint those in senior management positions;
- any individual(s) holding more than 25 percent of the Merchant's voting rights;
- any individuals (for example, the CEO) who hold senior management positions; and
- trustees (where applicable);

Forward Dated Risk means the credit risk associated with the PayFac/Aggregation service being provided to the Merchant taking into account the risk of Chargebacks/Disputes in respect of payments received in advance before the Merchant provides the goods or services;

FT means financing of terrorism;

General Manager Payments means XXXX or such other replacement or successor appointed by Venue Smart from time to time;

ISO means an entity that acts as an independent sales organisation on behalf of a Card Acquirer where the ISO resells the Card Acquirers payment service. The ISO typically has responsibility for signing up the Merchant to the Card Acquirers compliance and credit risk standards but does not underwrite the risk. The ISO typically receives the margin difference from the Card Acquirers ISO wholesale fee rate and the rate the ISO sells the payment service for;

Issuer means the issuing bank responsible for issuing the bank card (whether credit, debit or prepaid) to the cardholder;

Management Team means the General Manager Payments, the Venue Smart chief executive officer, the Venue Smart chief financial officer and XXXX;

Merchant means a Venue Smart customer that is approved to use the PayFac, Aggregation or ISO service;

ML means money laundering;

NPP (New Payments Platform) means that payment type, supplied by the bank, that allows a payer to pay a payee real time or a payee to debit a payer in real time using an NPP payment identifier;

PayFac means a payment facilitation service used to process card transactions provided by the Card Acquirer to Venue Smart and on-supplied by Venue Smart to Merchants;

Payments Operations Team means the group of staff appointed by Venue Smart to manage payment operations.

PCI DSS means the Payment Card Industry Data Security Standard introduced by the Schemes for the protection of cardholder data and the associated transactions.

PEP (politically exposed person) means:

a An individual who holds, or has held at any time in the preceding 12 months, in any overseas country the prominent public function of:

- Head of State or head of a country or government; or
- government minister or equivalent senior politician; or
- Supreme Court Judge or equivalent senior Judge; or
- Governor of a central bank or any other position that has comparable influence to the Governor of the Reserve Bank of Australia; or

- Senior foreign representative, ambassador, or high commissioner; or
- high-ranking member of the armed forces; or
- board chair, chief executive, or chief financial officer of, or any other position that has comparable influence in, any State enterprise; and

b. An immediate family member of a person referred to in paragraph (a), including:

- a spouse; or
- a partner, being a person who is considered by the relevant national law as equivalent to a spouse; or
- a child and a child's spouse or partner; or
- a parent; and

c. Having regard to information that is public or readily available:

- any individual who is known to have joint Beneficial Ownership of a legal entity or legal arrangement, or any other close relationship, with a person referred to in paragraph a; or
- any individual who has sole Beneficial Ownership of a legal entity or legal arrangement that is known to exist for the benefit of a person described in paragraph a;

Venue Smart means Venue Smart (ABN 52 604 254 766);

Venue Smart Risk Committee means the risk committee, comprised of XXXX including [Venue Smart's] Chief Financial Officer, at least 2 Board directors, [Venue Smart's] Chief Information Officer, the Compliance Manager and 1 independent payments compliance professional or such other members who are appointed as comprising the risk committee from time to time;

Venue Smart CRM means a web-based, customer relationship management system used by Venue Smart to serve as a central repository for customer records and Complaint handling;

Venue Smart Risk Management Framework means the risk management plan developed by Venue Smart from time to time detailing Venue Smart's risk management process and which is adopted by Venue Smart it's risk management framework;

Prescribed Transaction means a transaction conducted through the PayFac or Aggregator service in respect of:

- a domestic (i.e. within Australia) physical cash transaction of AUS$10,000 and over;

Prohibited Industry means a Merchant that operates within an industry that is prohibited by Venue Smart, the Card Acquirer, the Service Provider, legislation, card scheme rules, regulations or otherwise;

Prohibited Merchant means a Merchant that is prohibited from using the PayFac or Aggregator service by Venue Smart, the Card Acquirer, the Service Provider, legislation, card scheme rules, regulations or otherwise (refer to the Credit Risk Policy for more information on "Prohibited Merchants");

Refund means the returning of customer funds or fees where the request may be as a result of one (but not limited to) overcharging, charging a fee not in an agreement, non supply of goods or services, faulty supply of goods or services, service level failure or a breach of an agreement;

Resellers means those parties that develop business management software for an industry and have embedded the PayFac's payment processing capabilities within their business software. The Reseller also has an agreement with the PayFac to resell their services.

Risk Register means the register of risk maintained by the General Manager Payments;

Scheme (also Association) means an organisation that has created a card product or Scheme with associated rules and regulations for the issuance, acquiring and use of that product. Also known as a card Scheme. Typical card Associations/Schemes include, Visa, MasterCard, China UnionPay, JCB, Diners, Discovery and EFTPOS; and

Service Provider means that business that has the ability to supply Aggregated Direct Entry, NPP or BPay payments services to Venue Smart.

2.0 Introduction

Venue Smart Pty Ltd (Venue Smart) is a multi-channel payments processor offering merchants the ability to accept both online and across the counter payments (via an EFTPOS device). The service is called XXXX.

Venue Smart supports the following payment types online:

- Card (Visa and MasterCard debit and credit cards)
- BPay
- Direct debit and NPP payments

Venue Smart supports the following payment types across the counter via an EFTPOS device:

- online and card (Visa and MasterCard debit and credit card)
- proprietary EFTPOS cards).

The online payments facilities are provided by Global Payments.

The across the counter payments facilities are supplied by FiServ.

Venue Smart is 100% owned by XXXX.

To support the above payment types Venue Smart is required to operate as follows:

- Online Cards processing as a Payment Facilitator (PayFac)
- Across the counter EFTPOS processing as an Independent Sales Organisation (ISO)
- Direct debit/NPP processing as a Direct Entry/NPP Aggregator
- BPay processing as BPay Aggregator

As a PayFac Venue Smart is pre-issued card based Merchant ID's which are in-turn allocated by Venue Smart to a merchant. All funds are settled into the Card Acquirers owned and managed custodial account (in the name of Venue Smart) held at its bank. Venue Smart initiates disbursements from the custodial settlement account to the merchant's designated bank account.

As a Direct Entry/NPP and BPay Aggregator all funds are settled into a Venue Smart settlement account. Venue Smart initiates disbursements from the settlement account to the merchant's designated bank account.

As an ISO Venue Smart acts as a reseller of the Card Acquirer.

As a PayFac and Aggregator, Venue Smart absorbs the compliance and credit risks associated with servicing the merchant with a payment service.

As an ISO, the Card Acquirer absorbs the compliance and credit risks associated with servicing the merchant with a payment service.

Venue Smart has risks associated across the following broad areas:

- Regulatory
- Credit
- Financial and Market
- Strategic
- Operational
- Cyber Security & Privacy

This document is based on Venue Smart's AML/CFT risk assessment. In particular, it puts procedures, policies and controls in place to (i) detect and deter money laundering and terrorist financing (ii) ensure Venue Smart manages the inherent risks of money laundering and terrorist financing that Venue Smart has identified in its risk assessment and (iii) mitigates against the possibility of inadvertently assisting a third party from being able to money launder or finance terrorism.

Venue Smart has received advice that by offering the PayFac and Aggregator service, it is **NOT** a "reporting entity" under the AML/CFT Act and, as such, is **NOT** required to comply with the provisions of that Act.

Even though Venue Smart is by law **NOT** required to be registered with ASIC for an Australian Financial Services Licence (AFSL) **NOR** be a reporting entity for Austrac it has decided to follow the AML/CFT policies and processes required by an AusTrack reporting entity. These include:

- Staff being adequately trained in the prevention and detection of money laundering and the financing of terrorism;
- The establishment, implementation and maintenance of Venue Smart AML/CFT Policy that includes internal procedures, policies, and controls to:
    - detect money laundering and financing of terrorism; and
    - manage and mitigate the risk of money laundering and financing of terrorism; and
- The appointment of an AML/CFT compliance officer to administer and maintain Venue Smart's AML/CFT Policy.

Responsibility falls on the Board and Management Team to:

- Consider the money laundering and terrorist financing risks;
- Ensure that the systems that are in place are as adequate and effective as they can be to detect and deter money laundering and terrorist financing risk;
- Implement training programs to ensure that all staff understand Venue Smart's AML/CFT procedures, policies and controls and accordingly:
    - are suitably trained to understand the money laundering and terrorist financing risks associated with Venue Smart's business;
    - are able to detect and deter against instances, or suspected instances, of money laundering and terrorist financing;
    - take steps to mitigate against such risks materialising;
    - know how to recognise and deal with some example suspicious transactions and/or activities;
    - know when and how enhanced due diligence (EDD) will be undertaken;
    - know when and how to escalate PEP and sanction screening;
    - know when and how to escalate suspicious activity or Prescribed Transactions;
    - understand the relevant money laundering and terrorist financing legislation and, where relevant, AML/CFT supervisor guidance material (including new developments) applicable to Venue Smart's business and assist Venue Smart in complying with its obligations under the AML/CFT Act and the applicable regulations (i.e. conduct appropriate customer due diligence and/or report suspicious activity or Prescribed Transactions), collectively referred to as "Training Program Outcomes".

This document outlines the AML/CFT policy of Venue Smart.

3. Management and maintenance

This AML/CFT Policy will be managed and maintained on a day-to-day basis by the Compliance Manager.

The Compliance Manager:

- Is also designated as the anti-money laundering and countering the financing of terrorism compliance officer (AML/CFT Compliance Officer). In the Compliance Manager's absence [for a continuous period exceeding 5 business days], the Chief Financial Officer will be designated as the AML/CFT Compliance Officer until the Compliance Manager resumes their duties as AML/CFT Compliance Officer or is otherwise replaced by a new person appointed by Venue Smart to act as its AML/CFT Compliance Officer; and
- Will also assume the role as the anti-money laundering and countering the financing of terrorism reporting officer (AML/CFT Reporting Officer). The AML/CFT Reporting Officer must report to [to the CFO and Risk Committee].

4. Monitoring and review process

The Compliance Manager must administer and maintain this AML/CFT Policy and ensure that the AML/CFT Policy is:

- Provided to the Management Team 12 monthly for review to (i) ensure the AML/CFT Policy is up to date, (ii) identify any deficiencies in the effectiveness of the AML/CFT Policy and (iii), where appropriate, make any necessary changes;
- Kept in line with any guidance produced by Austrac or the finding of any independent auditor/reviewer;
- Reviewed and approved by the Board on an annual basis; and
- Audited every 2 years (or at any other time at the request of the Card Acquirer or the Service Provider) by an independent and appropriately qualified reviewer.

The Compliance Manager must also:

- Fulfill his or her responsibilities as set out in this AML/CFT Policy;
- Maintain their AML/CFT awareness by attending training events and keeping a watching brief on the media as well as publications and guidance published by Venue Smart's AML/CFT supervisor and other relevant bodies;

- Monitor and manage compliance by all staff with attending training procedures, policies and controls and is also responsible for internal communication of and training in, those procedures, policies and controls;
- Investigate any suspicious activities and advise staff on the next course of action;
- Ensure that appropriate suspicious activity reports and Prescribed Transaction reports are submitted in a timely manner;
- Make records relating to this AML/CFT Policy (including any audit of this AML/CFT Policy) available to the Card Acquirer or Service Provider on request; and
- Prepare and submit an annual report to Venue Smart's Board

The General Manager, Payments must:

- Ensure the AML/CFT Policy is operationally implemented (i.e. that Venue Smart's staff adhere to the internal procedures, policies and controls recorded in this AML/CFT Policy including the customer/Merchant due diligence processes); and
- Report daily and monthly to the Compliance Manager, Venue Smart's status against the AML/CFT Policy. The report is to take the form of updates to the AML/CFT Risk Register.

5.0 Vetting and Training

5.1. Vetting checks and training generally

Venue Smart undertakes a comprehensive staff recruitment, vetting, onboarding and training program and acknowledges that all staff (irrespective of their position and role) have an element of risk management and risk mitigation as part of their job description. This includes the below persons as required by the AML/CFT Act:

- All Venue Smart senior management who may be in a position to influence the management or administration of the Venue Smart business or decide and/or override decisions concerning a Merchant, or services/products if a new service/product is introduced (i.e. CEO, CFO and CRO);
- The AML/CFT Compliance Officer;
- The Payments Operations Team; and
- Any other member of staff whose role involves anti-money laundering and terrorist financing risks.

For this reason, all staff are:

- Vetted to mitigate the risk of hiring someone who may use Venue Smart's business for money laundering and terrorist financing;
- Inducted on risk relevant to their roles upon starting within the business;
- Assessed against their risk management as part of their key performance indicators; and

- Trained regularly on risk relevant to their roles.

5.2 New staff vetting:

Venue Smart may make a conditional offer of employment prior to the completion of the vetting checks; however, this offer is subject to the vetting checks having a satisfactory result and being successfully completed. These vetting checks include that all staff members:

- Are reference checked by obtaining at least two employment reference checks (not required for staff with no prior working experience) and/or character references (as applicable);
- Are police checked (except overseas applicants who have a valid Australian visa);
- Are checked to identify if they or any of their relatives are PEPs or any legal entity or legal arrangement they are associated with has any PEPs within their ownership structure or are otherwise subject to any sanctions;
- Are checked to identify whether the prospective staff member has any secondary business interests that may present money laundering and/or terrorist financing risk;
- Provide a copy of the prospective staff member's passport and visa (if required) or other acceptable form of identity document;
- Provide a copy of the prospective staff member's proof of physical address (i.e. a utility bill or bank statement issued within the last 3 months of the date of providing the same);
- Are appropriately experienced and trained;
- Have a job description with the appropriate risk mitigation key performance indicators; and
- Are reviewed annually for performance.

5.3 Vetting or re-vetting of existing staff (as applicable)

Any existing staff who have not been vetted as set out in section 5.2 above will be vetted in accordance with this AML/CFT Policy – the intention being that vetting of all such staff will be completed prior to XXXX.

5.4 Ongoing vetting of staff

Where any staff member:

- Transfers or is promoted into a higher-risk role within Venue Smart (i.e. director, an executive, the Compliance Manager, the Payments Operations Team etc.);
- Has been in a high-risk role for a period of [3 years];
- Is the subject of any adverse media indicating potential involvement in, or association with, known criminals or criminal activity;

- Fails to comply with this AML/CFT Policy in any material respect (by way of example, fails to conduct appropriate due diligence on a Merchant or fails to escalate any suspicious activity or Prescribed Transactions to the Compliance Manager), or
- The Compliance Manager (in his/her sole and unfettered discretion) considers it necessary that a member of staff should be re-vetted then, in each case, that staff member must be re-vetted as set out in section 5.2.

5.5 Personnel completing vetting:

Where vetting of staff is done internally by employees or externally by third parties (as the case may be), Venue Smart is satisfied that those people have the appropriate skills and experience to perform these checks.

5.6 Training

Venue Smart's training programs are designed to ensure that all staff:

- have received sufficient training on each aspect of the Training Program Outcomes;
- understand how they will be assessed by [Venue Smart] against their key performance indicators; and
- sign a register, at least annually, confirming that (in the staff member's opinion) they have received sufficient training on, and understand, each aspect of the Training Program Outcomes.

The risk documents are accessible by the relevant staff within the Venue Smart repository.

5.7 Scope and nature of training

Venue Smart develops staff AML/CFT training and associated materials to cover each aspect of the Training Program Outcomes under the leadership of the Board and Management Team in conjunction with regulatory guidance, third party providers and other subject matter experts as appropriate.

5.8 How AML/CFT training is applied

All staff must undergo Venue Smart's AML/CFT training that covers each aspect of the Training Program Outcomes at least annually.

New staff are required to complete Venue Smart's AML/CFT training within 3 months of commencing employment.

All staff must sign a register, at least annually, confirming that (in the staff member's opinion) they have received sufficient training on, and understand, each aspect of the Training Program Outcomes.

Certain staff may be required by the Compliance Manager to undergo more frequent training where there has been an instance (or repeated instances) of non-compliance with Venue Smart's AML/CFT practices (i.e. where a capability or competency gap is identified).

Key performance assessments of staff and associated wages/salaries may be impacted if staff do not complete the required training. In severe cases of non-compliance staff may commit misconduct, serious misconduct or material breach of contract, which may result in disciplinary action culminating in termination of employment (including summary dismissal) or termination of contract.

6.0 AML/CFT Policy

Venue Smart's risk assessment records that Venue Smart's inherent money laundering and financing of terrorism risk rating is moderate to low but that does not mean that there is no risk.

The purpose of the AML/CFT Policy is to detect money laundering and the financing of terrorism and manage and mitigate the risk of money laundering and financing of terrorism as recorded in the risk assessment. One of the ways in which Venue Smart achieves this is by undertaking the necessary steps to identify its customers and verify they have not been sanctioned and/or that they are not a PEP.

This process is called "Know Your Customer" (KYC) or "Customer Due Diligence" (CDD). This AML/CFT Policy identifies the minimum CDD requirements and the processes to be undertaken to ensure these standards are managed.

7.0 Payments Operation Team **(operating as the AML/CFT Team)**

The Payments Operations Team must manage the AML/CFT processes on a day-to-day basis and report to the General Manager, Payments.

All members of the Payments Operations Team should:

- Be reference checked;
- Be police checked;
- Be appropriately experienced in AML/CFT processes and trained;
- Have a job description with the appropriate risk mitigation key performance indicators;
- Be reviewed annually for performance;
- Be trained every 6 months on Venue Smart's AML/CFT policies, processes and procedures;

- Sign a register, at least annually, confirming that (in the staff member's opinion) they have received sufficient training on, and understand, each aspect of the Training Program Outcomes.

The Payments Operations Team, from time to time, may engage third party suppliers to assist in the collection of KYC data, sanction screening and PEP screening. Any supplier engagement must be approved by the Compliance Manager. The Compliance Manager must ensure the supplier meets all the AML/CFT procedures set out in this AML/CFT Policy or as otherwise directed by the Card Acquirer from time to time.

8.0. Regulatory Requirements - customer due diligence (CDD)

8.1 Introduction

As a general rule, Venue Smart does not undertake simplified CDD under the AML/CFT Act because Merchants are unlikely to satisfy the circumstances when simplified CDD applies. The Payments Operations Team is therefore required to undertake standard CDD on each Merchant and, in some cases, enhanced due diligence (EDD) as set out in section 9. This includes:

- Obtaining all relevant identity and proof of address documentation (as required under this AML/CFT Policy);
- Taking reasonable steps to satisfy itself that the information obtained during the CDD process is correct;
- Taking reasonable steps, according to the level of risk involved, to verify any Beneficial Owner's identity so that the reporting entity is satisfied that it knows who the Beneficial Owner is and is able to make appropriate decisions about the level of money laundering and terrorist financing risk presented by the Merchant;
- Where a person is acting on behalf of the Merchant (i.e. a director, authorised signatories or agent of the Merchant), taking reasonable steps, according to the level of risk involved, to verify that person's identity and authority to act on behalf of the Merchant so that Venue Smart / the Payments Operations Team is satisfied it knows who the person is and that the person has authority to act on behalf of the Merchant;
- Obtaining information on the nature and purpose of the proposed business relationship between the Merchant and Venue Smart or as otherwise necessary to determine whether the Merchant should be subject to EDD – this could include the reason the Merchant would like to use the PayFac/Aggregation service, the estimated total dollar value that may be processed through the PayFac/Aggregation service by the Merchant per annum and/or information on the expected pattern, level, and type of activity (i.e. transaction volumes and frequency);

- Where possible, making reasonable enquiries of each Merchant to determine whether the Merchant is a bona fide business engaged in arms-length commercial activities with its patients/customers;
- Where possible, making reasonable enquiries of each Merchant or through publicly available registers to determine whether the Merchant is licenced and/or registered with all relevant authorities for its business type;
- Taking such steps as may be appropriate and reasonable in the circumstances to be satisfied that each transaction processed through the PayFac or Aggreator is or will be a true reflection of the commercial relationship between the Merchant and the payer];
- Satisfying itself that the Merchant is not a Prohibited Merchant and/or is not operating within a Prohibited Industry; and
- Satisfying itself that the Merchant operates within Australia.

The Merchant data to be collected for verification varies depending on the customer/Merchant type. Below is listed each customer/Merchant type and their associated verification data sets.

For the purposes of the following sections "person(s) acting on behalf of the Merchant" include those persons in sufficiently senior roles who have authority to engage with Venue Smart in respect of the relationship between the Merchant and Venue Smart.

8.2 Individual/Sole Traders/General Partners

The Payments Operations Team is required to collect the following key data on an Individual or sole trader or general partnership Merchant before it is issued with a PayFac or Aggregator service.

KYC Customer Data Collection Requirements	**Acceptable forms of verification**
Full name	One of the following: ● Drivers licence ● Passport ● Identity report by a recognised KYC bureau
Date of birth	One of the following: ● Drivers licence ● Passport ● Identity report by a recognised KYC bureau
Residential address (PO Box is not acceptable)	One of the following: ● Drivers licence ● Utility bill (less than 6 months old)

	● Bank statement (less than 6 months old) ● Identity report by a recognised KYC bureau
Principal place of business	One of the following: ● Rental agreement (current) ● Title deed ● Medicare letter (less than 6 months old) ● Tax letter/bill (less than 6 months old) ● Utility letter/bill (less than 6 months old) ● Bank letter/statement (less than 6 months old) ● Identity report by a recognised KYC bureau
Australian Business Number (ABN)	One of the following: ● Australian Business Number (ABN) look up report ● Identity report by a recognised KYC bureau
Business or Trading Name	One of the following: ● Australian Securities and Investments Commission (ASIC) look up report ● ABN look up report ● Identity report by a recognised KYC bureau
Nature and purpose of the proposed business relationship between the Merchant and Venue Smart, if this is not immediately clear and obvious to the Payments Operations Team.	A general description provided by the Merchant (if required).

Note:

- If a Merchant is an individual (and there are no reasonable grounds to suspect that the individual is acting on behalf of another person) the AML/CFT Act allows Venue Smart to treat that person as the Beneficial Owner. If the individual is acting on behalf of another person, it will be necessary to establish that person's identity, the Beneficial Ownership of the Merchant and any other Beneficial Owners; and
- Where the Merchant is 'high risk', resides in a 'high-risk' jurisdiction, has Beneficial Ownership in a 'high-risk' jurisdiction, or has been identified as a PEP or has Beneficial Ownership that has been identified as a PEP, EDD will be required. If certain information is unavailable, an identification report by a recognised KYC bureau (issued

within the last 3 months) may be used to supplement the information required by the above table.

8.3 Companies

The Payments Operations Team is required to collect the following key data on a company Merchant before it is issued with a PayFac or Aggregator Service.

KYC Data Collection Requirements	**Acceptable forms of verification**
ASIC registered entity name	One of the following: ● ASIC look up report ● ABN look up report ● Company identification report by a recognised KYC bureau
Registered address of the Australian office	One of the following: ● ASIC look up report ● ABN look up report ● Company identification report by a recognised KYC bureau
Australian Company Number (ACN), Australian Registered Body Number (ARBN) or Australian Business Number (ABN)	One of the following: ● ASIC look up report ● ABN look up report ● Company identification report by a recognised KYC bureau
Whether the company is registered as a Proprietary or Public Company	One of the following: ● ASIC look up report ● ABN look up report ● Company identification report by a recognised KYC bureau
Business or Trading Name	One of the following: ● ASIC look up report ● ABN look up report ● Company identification report by a recognised KYC bureau
Principal place of business	One of the following: ● Rental agreement ● Title deed ● Medicare letter (no older than 6 months) ● Tax letter/bill (no older than 6 months) ● Utility letter/bill (no older than 6 months)

	● Bank letter/statement (no older than 6 months) ● Identity report by a recognised KYC bureau
Identification Information on all key individuals: i.e ● Directors ● Authorised individuals instructing Venue Smart	One of the following: ● ASIC look up report ● Company identification report by a recognised KYC bureau ● See Section 8.2 for the identification data to be collected on each key individual
Identification information on all Beneficial Owners* *Note: The Payments Operations Team should establish and understand the Merchant's ownership structure at each layer. The Beneficial Owner is not necessarily one individual; there may be several Beneficial Owners in a structure. Where there are complex ownership layers with no reasonable explanation, the Payments Operations Team should consider the possibility that the structure is used to hide the Beneficial Owner(s). If so, EDD may be required.	One of the following: ● ASIC look up report ● Company identification report by a recognised KYC bureau ● See Section 8.2 for the identification data to be collected on each key individual
If the company is registered overseas then all relevant international company registration details	One of the following: ● Copy of foreign company registration details ● Search of publically accessible registers maintained by the local regulator.
Nature and purpose of the proposed business relationship between the Merchant and Venue Smart, if this is not immediately clear and obvious to the Payments Operations Team.	A general description provided by the Merchant (if required).

8.4 Partnerships

The Payments Operations Team is required to collect the following key data on any partnership Merchant before that Merchant is approved to use the PayFac or Aggregator Services.

KYC Data Collection Requirements	Acceptable forms of verification
Full name of partnership	One of the following: ● ASIC look up report ● ABN look up report ● State authority look up report ● Company identification report by a recognised KYC bureau
Full ASIC or state body registered business name (if any)	One of the following: ● ASIC look up report ● ABN look up report ● State authority look up report ● Company identification report by a recognised KYC bureau
Country partnership was established	One of the following: ● ASIC look up report ● ABN look up report ● State authority look up report ● Rental agreement (less than 6 months old) ● Title agreement ● Company identification report by a recognised KYC bureau
Australian Business Number	One of the following: ● ABN look up report ● Company identification report by a recognised KYC bureau
Identification Information on all key individuals: i.e ● Partners ● Authorised individuals instructing Venue Smart	One of the following: ● ASIC look up report ● Company identification report by a recognised KYC bureau ● See Section 8.2 for the identification data to be collected on each key individual
Identification information on all Beneficial Owners* *Note: The Payments Operations Team should establish and understand the Merchant's ownership structure at each layer. The Beneficial Owner is not necessarily one individual; there may be several Beneficial Owners in a structure. Where there are complex ownership layers with no reasonable explanation, the Payments	One of the following: ● ASIC look up report ● Company identification report by a recognised KYC bureau ● See Section 8.2 for the identification data to be collected on each key individual

Operations Team should consider the possibility that the structure is used to hide the Beneficial Owner(s). If so, EDD may be required.	
Australian Business Number (ABN)	One of the following: ● ASIC look up report ● ABN look up report ● Company identification report by a recognised KYC bureau
Nature and purpose of the proposed business relationship between the Merchant and Venue Smart, if this is not immediately clear and obvious to the Payments Operations Team.	A general description provided by the Merchant (if required).

Note:

- If a partner is an individual (and there are no reasonable grounds to suspect that the individual is acting on behalf of another person), the AML/CFT Act allows Venue Smart to treat that person as the Beneficial Owner. If the individual is acting on behalf of another person, it will be necessary to establish that person's identity, the Beneficial Ownership of the Merchant partner and any other Beneficial Owners;
- Where the Merchant partnership is 'high risk' or where a partner resides in a 'high risk' jurisdiction, or has an individual partner or a trust with a Beneficial Owner residing in a 'high-risk' jurisdiction or is otherwise identified as a PEP, EDD will be required. If certain information is unavailable, an identification report by a recognised KYC bureau (issued within the last 3 months) may be used to supplement the information required by the above table.

8.5 Associations

The Payments Operations Team is required to collect the following key data on an association Merchant before it is issued with a PayFac or Aggregator Service.

KYC Data Collection Requirements	**Acceptable forms of verification**
Full name of association	One of the following: ● ASIC look up report ● State authority look up report ● Constitution ● Company identification report by a

	recognised KYC bureau
Full address of principal place of business or administration	One of the following: ● ASIC look up report ● State authority look up report ● Constitution ● Company identification report by a recognised KYC bureau
Unique identification number allocated to the association on its incorporation	One of the following: ● ASIC look up report ● State authority look up report ● Constitution ● Company identification report by a recognised KYC bureau
Australian Business Number (ABN)	One of the following: ● ABN look up report ● Company identification report by a recognised KYC bureau
Identification data of all key individuals, i.e. ● Beneficial Owners ● Office bearers ● A member (if the association is unincorporated)	One of the following: ● ASIC look up report ● Company identification report by a recognised KYC bureau ● See Section 8.2 for the identification data to be collected on each key individual

8.6 Government Bodies

The Payments Operations Team is required to collect the following key data on a Merchant controlled/owned by a government body before that Merchant is approved to use the PayFac or Aggregator service.

KYC Data Collection Requirements	**Acceptable forms of verification**
Full name of government body	One of the following: ● Company identification report by a recognised KYC bureau
Full address of principal place of business	One of the following: ● Rental agreement ● Title deed ● Company identification report by a

	recognised KYC bureau
Is the government body a entity, emanation or established under legislation	One of the following: ● Individual identification report by a recognised KYC bureau
Australian Business Number (ABN)	One of the following: ● ABN look up report ● Company identification report by a recognised KYC bureau
Is the government body foreign owned	One of the following: ● Reliable source document of body set up, registration, address etc.
Collection of key individuals' information, being any person(s) or employees with the authority to act on behalf of the government body Merchant who will provide instructions to Venue Smart (however, please note this is not required for a government body that is a major shareholding entity with >25% ownership of a Merchant).	See Section 8.2 for the identification data to be collected on each key individual

8.7 Trusts

The Payments Operations Team is required to collect the following key data on a trust Merchant before it is issued with a PayFac or Aggregator service.

KYC Data Collection Requirements	**Acceptable forms of verification**
Full name of trust	A copy of the trust deed and any amendments to the trust deed (including deeds of appointment) or an extract of the trust deed, showing: ● the name of the trust; ● date of establishment; ● names of the settlor(s), trustee(s), appointor(s), protector(s), beneficiaries or classes of the beneficiaries.
Full business name (if any) of trust	
Type of trust	
Country in which trust was established	
Full name of settlor of trust	
Full names of trust beneficiaries or a description of each class of beneficiary	
Physical address of the trust	Proof of physical address in the name of the trust

Full name of Trustee/s including professional trustees; trustee companies and their directors	Please refer to above 8.2 above for what information to collect for each key individuals in relation to verifying the full name, date of birth and address of each key individual, and to 8.3 (and 8.3 in an instance where the trustee(s) are a trustee company).
All individuals with the power to alter the trust deed, or the power to appoint or remove trustees (including but not restricted to appointors, settlors and protectors).	Please refer to above 8.2 above for what information to collect for each key individuals in relation to verifying the full name, date of birth and address of each key individual.

Note: Where certain information is unavailable, an identification report by a recognised KYC bureau (issued within the last 3 months) may be used to supplement the information required by the above table.

8.8 Registered Co-operatives

The Payments Operations Team is required to collect the following key data on a co-operative Merchants before it is issued with a PayFac or Aggregator service.

KYC Data Collection Requirements	**Acceptable forms of verification**
Full name of registered co-operative	One of the following: ● ASIC look up report ● State registration report ● Copy of co-operative register ● Copy of minutes from a co-operative meeting ● Company identification report by a recognised KYC bureau
Australia Business Number (ABN)	One of the following: ● ABN look up table ● Company identification report by a recognised KYC bureau
Identification data on key individuals, i.e: ● Association office bearers, i.e. Chairman, Secretary, Treasurer or equivalent	One of the following: ● ASIC look up report ● Copy of co-operative register

● Beneficial Owner ● Any authorised individual who can instruct Venue Smart	● Individual identification report by a recognised KYC bureau ● See Section 8.2 for the identification data to be collected on each key individual
Full address of principal place of business	One of the following: ● Rental agreement ● Title deed ● Company identification report by a recognised KYC bureau
Unique identification number allocated to the co-operative	One of the following: ● ASIC look up report ● State registration report ● Copy of co-operative register ● Copy of minutes from a co-operative meeting ● Company identification report by a recognised KYC bureau

9.0 Enhanced Due Diligence (EDD)

9.1 Key distinction between EDD and standard CDD

EDD has two core requirements over and above standard CDD:

- Venue Smart may need to use increased or more sophisticated measures to obtain and verify a Merchant's details, their Beneficial Ownership structure, and the details of representatives and other key persons. Venue Smart is required to take reasonable steps to do this according to the level of risk involved; and
- Venue Smart should usually obtain and verify information relating to the source of wealth (i.e. the origin of the Merchant's entire body of assets) (**SoW**) or source of funds (i.e. the origin of the funds used for the transactions or activities that occur within the business relationship with Venue Smart) (**SoF**) of its Merchant.

9.2 When EDD is required

The Payments Operations Team is required to undertake an EDD process for Merchants where:

- The Merchant is a trust or another vehicle for holding personal assets;
- The Merchant or any Beneficial Owner of the Merchant is a non-resident customer from a country that has insufficient anti-money laundering and countering financing of

terrorism systems or measures in place – the Countries Assessment Guideline will help to determine which countries have insufficient AML/CFT measure in place;

- The Merchant is a company with some or all of its share in bearer form (i.e. where ownership of the shares is based on who physically holds the share certificate) or where some or all of the company's shareholders are nominee shareholders;
- It is determined under Venue Smart's credit risk policy and/or Venue Smart's risk assessment that the Merchant is high risk;
- The Merchant seeks to conduct, through Venue Smart and/or PayFac/Aggregation facility, a complex, unusually large transaction or unusual pattern of transactions that have no apparent or visible economic or lawful purpose;
- Venue Smart wishes to establish a business relationship with a Merchant or a Merchant seeks to conduct an occasional transaction or activity through Venue Smart and/or the PayFac/Aggregation facility that involves new or developing technologies, or new or developing products, that might favour anonymity or enable obscured Beneficial Ownership;
- where the Merchant or any Beneficial Owner of the Merchant is a PEP;
- A suspicious matter has arisen which might require Venue Smart to make a suspicious activity report:
    - during the merchant sign up/on-boarding process; or
    - during the course of doing business with the Merchant.

9.3 Purpose of EDD

The EDD process requires the Payments Operations Team to establish a reasonable confirmation or understanding of:

- Whether complex Beneficial Ownership structures are legitimate and intended to facilitate business or if they are deliberately complicated to hinder investigation and conceal the identity of the Beneficial Owners;
- Whether a Merchant's SoW or SoF are legitimately derived, or intended for legitimate use, or whether there are reasonable grounds to suspect it may be the proceeds of crime;
- Whether a Merchant is likely to be engaged in transactions or activities that may be linked to money laundering and terrorist financing;
- Whether a Merchant is involved in suspicious activity that needs to be reported to the FIU;
- Country of citizenship or residence of Beneficial Owners; and
- Negative/derogatory information related to the Merchant business or owners.

9.4 EDD re-verification

In some cases it may be necessary for the Payments Operations Team to conduct EDD again for existing Merchants. The re-verification may be necessary where:

- The data previously supplied appears to be inconsistent or have discrepancies (i.e. there are doubts about the adequacy or veracity of the information, data and documents that were previously obtained and verified in relation to that Merchant);
- The transactions processed appear to be high risk;
- Due to Venue Smart's ongoing CDD and account monitoring processes, Venue Smart / the Payments Operations Team identifies that there are, or have been, material changes in Venue Smart's business relationship with a particular Merchant. Examples of material changes include situations where:
    - there are inconsistencies between what Venue Smart knows about a Merchant and the transactions and activities that the Merchant conducts;
    - the nature and purpose of the business relationship has changed to an extent that could present an increased money laundering or financing of terrorism risk;
    - the Merchant has changed its ownership structure through new corporate or trust structures; or
    - a review of a low- or medium-risk Merchant's account activity and transaction behaviour shows that their risk level of money laundering and terrorist financing has increased since Venue Smart's previous assessment beyond what is reasonably expected or usually processed.

9.5 Additional EDD actions

Where Venue Smart is required to undertake EDD the Payments Operations Team should consult with the Compliance Manager to seek the appropriate course of action. In addition to conducting CDD in accordance with Section 7 above, additional due diligence actions will be required including:

- Taking reasonable steps to verify that information, data, or documents supplied by Merchants for verification of identity purposes are issued by a reliable and independent sources;
- Taking reasonable steps, according to the level of risk involved, to verify the Merchant's SoF or SoW using documents, data or information issued by a reliable and independent source. To identify the SoW or SoF of a trust, the Payments Operations Team will need to identify the individual(s) who are the settlor(s), the origin of the settlor's wealth and (if relevant) the source of any income that the trust is receiving. The Payments Operations Team is not expected to account for every part of a Merchant's SoW or SoF. However, the Payments Operations Team must be satisfied that the nature and size of a

Merchant's wealth matches what the Payments Operations Team knows about that Merchant. Whilst the Payments Operation Team can use its judgment on the level of verification to be used depending on the situation, the Merchant, activity or transaction, the steps that the Payments Operation Team takes should be objective, appropriate for Venue Smart's business and proportionate with the level of money laundering and terrorist financing risk. In general, the following documents, data, or information could be considered reliable and independent:

- Government-issued or registered documents or data from a low-risk country with sufficient AML/CFT measures;
- Full bank and other investment statements;
- Full payslip or wage slip or other documents confirming salary;
- GST number and IRD statement of earnings from the most recent year (for sole traders);
- Inheritance (stamped grant of probate, stamped grant of letters of administration);
- Audited financial accounts from a chartered accountant;
- Sales and purchase agreements.

Documentation accepted to verify SoW or SoF should depend on the level of money laundering and terrorist financing risk presented by the Merchant. The higher the risk, the more comprehensive and reliable documents obtained should be.

- In the case of a Merchant that is a trust (other than discretionary or charitable trust or a trust that has more than 10 beneficiaries), the name and the date of birth of each beneficiary of the trust – note that there is no requirement to verify this information;
- In the case of a Merchant that is a discretionary or charitable trusts or a trust that has more than 10 beneficiaries, a description of:
  - each class or type of beneficiary; and
  - if the trust is a charitable trust, the objects of the trust.
- any additional information prescribed, from time to time, by regulations.

In exceptional circumstances, Venue Smart is permitted to complete delayed verification of Merchant identity for both standard CDD and enhanced CDD (**Delayed Verification**). Any proposal to undertake Delayed Verification must be authorised in writing by the Compliance Manager provided the Compliance Manager is satisfied that:

- the Merchant in question is not high risk;
- there are no reasonable grounds to suspect that the Merchant is likely to be engaged in transactions or activities that may be linked to money laundering and terrorist financing;

- Delayed Verification is necessary in the circumstances having regard to the AML/CFT Act and being satisfied that each element of the Act, or will be, complied with.

9.6 Ongoing CDD and account monitoring

The Payments Operations Team must regularly:

- review information about the business relationships Venue Smart has with Merchants; and
- conduct account monitoring which involves reviewing account activity and transaction behavior.

Note: The Credit Risk Policy requires the Payments Operations Team to conduct a review of all Merchants at least every 12 months.

If due to ongoing CDD and account monitoring processes, Venue Smart / the Payments Operations Team identifies that there are, or have been, material changes in Venue Smart's business relationship with a particular Merchant then this must be escalated to the Compliance Manager and the Payments Operations Team must conduct EDD on the Merchant. Examples of material changes include situations where:

- there are inconsistencies between what Venue Smart knows about a Merchant and the transactions and activities that the Merchant conducts;
- the nature and purpose of the business relationship has changed to an extent that could present an increased money laundering or financing of terrorism risk;
- the Merchant has changed its ownership structure through new corporate or trust structures; or
- a review of a low- or medium-risk Merchant's account activity and transaction behaviour shows that a Merchant's risk level of money laundering and terrorist financing has increased since Venue Smart's previous assessment beyond what is reasonably expected or usually processed.

Ongoing CDD and account monitoring assists Venue Smart / the Compliance Manager and staff with identifying suspicious activity which may give rise to a suspicious activity report or transactions for which Prescribed Transaction reports are required.

The Payments Operations Team should consider reviewing CDD (including enhanced CDD) for higher risk Merchants more regularly than for lower risk Merchants.

10. Regulatory Requirements - Sanction and PEP screening requirement

10.1 Sanctions

The Payments Operations Team must take reasonable steps to undertake sanction screening of the Merchant. The screening is to be against the following sanctions list:

- OFAC
- SDN
- DFAT
- UN

If an individual is applying to conduct a transaction through Venue Smart or the PayFac/Aggregation service then the sanction screening must be on the individual.

If a business is applying to conduct a transaction through Venue Smart or the PayFac/Aggregation service then the sanction screening must include the following:

- Beneficial Owners of the business;
- All persons acting on behalf of the Merchant (i.e. directors or agents); and
- Authorised signatories to the facility.

Where a Merchant, any Beneficial Owner, person acting on behalf of a Merchant or authorised signatory is, or is, associated with a sanctioned individual then:

- if the Merchant is an existing customer, the relevant Merchant's ability to process transaction through the PayFac/Aggregation facility must immediately cease; and
- if no business relationship has been established, the Merchant application must be rejected.

10.2 Politically Exposed Persons (PEP)

To put it briefly, a PEP is an individual, who in the last 12 months, has held a prominent overseas public position or function. The term PEP includes their relatives and close associates. It also includes people who have Beneficial Ownership of legal entities or arrangements existing to benefit PEPs. Due to their role, they may be more susceptible to bribery, corruption or other money laundering offences, as a result of this they are deemed to be of high risk.

If an individual is identified as a PEP, this does not mean that they are involved in criminal activity, but it means that precautions may need to be taken as they are of higher risk.

The Payments Operations Team must take reasonable steps to undertake PEP screening of a Merchant to determine if there are any PEPs engaged in or with a Merchant. The screening must include the following individuals involved with the entity:

- All Beneficial Owners
- Authorised signatories

According to the level of risk involved, it may be appropriate for the Payments Operations Team (as part of EDD) to use internet/media searches and publicly available reports to check if the Merchant, an authorised signatory of a Merchant or their Beneficial Owner is a PEP, especially when they are from a country with high levels of bribery, corruption, and organised crime. With larger or more complex businesses, the Payments Operations Team should (in consultation with the Compliance Manager) consider using the services of a third-party provider and commercially available databases to screen for PEPs.

Where an individual associated with the Merchant is deemed to be a PEP then:

- The Merchant application must be forwarded to the Compliance Manager for review and the Compliance Manager must decide whether to approve continuing the business relationship with the Merchant is question; and
- The Payments Operations Team must obtain and take reasonable steps to verify the PEP's SoW or SoF.

Key EDD questions that the Payments Operations Team should consider include:

- Whether the PEP's transaction/activity is in line with expectations?;
- Whether the PEP's identity data, address, employment, SoW or SoF and relatives and close associates' status is up to date?;
- Whether there are any unexplained changes to the PEP's details?;
- Whether the PEP's net worth has grown substantially in a short amount of time and if there is a clear explanation for the sudden growth?;
- Whether it is necessary to seek clarification from the PEP and update their details?

11. Products and services that favour anonymity

Venue Smart does not use products, provide services or engage in transactions that might favour anonymity.

Venue Smart addresses the risk of Merchant anonymity with regards its current services, use of technology and delivery methods, through the CDD policies, procedures and controls recorded

in this AML/CFT Policy and does not conduct a business relationship with anyone, or allow anyone to conduct an occasional transaction or activity through Venue Smart and/or the PayFac/Aggregation service, that does not meet the customer identification and verification requirements recorded in this AML/CFT Policy.

If Venue Smart identifies that its service, or a technology or delivery method it currently uses, favours anonymity in a previously unknown way, Venue Smart, with input and approval from the Compliance Manager, will:

- Update its risk assessment;
- Review and update this AML/CFT Policy to mitigate this risk to the extent possible;
- Redesign the service, use of technology or delivery method, to the extent possible, if the risk cannot be mitigated; and
- Review relevant Merchant transactions and activities to ascertain whether further action e.g., submitting a suspicious activity report, if necessary.

12. Reporting, record keeping and monitoring

12.1 General

The Payments Operations Team is required to report to the [Compliance Manager] on a daily and monthly basis the following:

- Merchant applications currently in the system:
    - Merchant name
    - Merchant type (individual/sole trader, company, limited partnership, partnership, , trust, government body,)
    - KYC data captured and results: - i.e. awaiting data, data ok, data not ok, to be reviewed by Compliance Manager
    - Other documents captured
    - Sales person name and contact details
    - Payments Operations Team member responsible
    - Screening results, i.e.
        - Approved
        - Declined - with reason
        - In progress
        - Undertaking EDD
        - To be reviewed by Compliance Manager due to:

- the Merchant or any legal entity or legal arrangement that the Merchant is associated with having PEPs within its ownership structure
- a positive sanction screen
- Payments Operations Team deems the application to be unusual and wishes to seek clarification

12.2 Record keeping

Venue Smart / the Payments Operations Team is required to file (either in paper or in electronic form) all the information, data or documents:

- In relation to every transaction that is conducted through Venue Smart or the PayFac/Aggregation service, all records that are reasonably necessary to enable that transaction to be readily reconstructed at any time including:
    - the nature of the transaction;
    - the amount of the transaction and the currency in which it was denominated;
    - the date on which the transaction was conducted;
    - the parties to the transaction;
    - if applicable, the facility through which the transaction was conducted, and any other facilities (whether or not provided by Venue Smart) directly involved in the transaction;
    - the name of the officer or employee or agent of Venue Smart who handled the transaction, if that officer, employee, or agent has face-to-face dealings in respect of the transaction with any of the parties to the transaction and has formed a suspicion about the transaction; and
    - any other information prescribed by regulations;
- Relevant to the establishment, or nature and purpose, of a business relationship with a Merchant;
- Relating to risk assessments, AML/CFT programmes, and audits;
- That the Payments Operations Team used to identify and verify each person's identity and details, their Beneficial Ownership (if applicable) and their SoW or SoF (if applicable) or otherwise reasonably necessary to enable the nature of the evidence used for the purposes of that identification and verification to be readily identified at any time ;
- Any other records prescribed by regulation.

Note: The Payments Operations Team should keep written notes or findings:

- that justify the level of verification undertaken by it and the reasons behind its AML/CFT decisions. For example, the Payments Operations Team should record

the reasons why Delayed Verification was permitted, or why it escalated, or chose not to escalate, a transaction monitoring alert to a suspicious activity report after conducting EDD;
    - of any complex or unusually large transactions;
    - of any unusual patterns of transactions with no obvious economic or lawful purpose;
    - of any business relationships and transactions from or in countries that do not have or have insufficient anti-money laundering or countering financing of terrorism systems in place; and
    - any other activity that is particularly likely, by its nature, to be related to money laundering or the financing of terrorism.
- All record keeping should be clear and logical so that another party reading the notes can understand the risk-based decision that was made. This is particularly important for supervisory and audit purposes.
- All electronic records should be backed up on a daily basis
- All paper records are to be stored in a locked cabinet
- All records should be kept for 7 years after the Merchant has ceased being a customer of Venue Smart

The Compliance Manager is to review **1 in 10** Merchant applications at the end of each month for compliance to the AML/CFT policy.

Unless there is a lawful reason for retaining the above records, the Payments Operations Team must take all practicable steps to ensure that every record retained by the Payments Operations Team under this AML/CFT Policy, and every copy of that record, is destroyed as soon as practicable after the expiry of the 7 year retention period.

12.3 CDD and prohibitions:

If the Payments Operations team is unable to conduct or complete CDD (including, where applicable, Delayed Verification or EDD) for a Merchant for reasons outside of its control (i.e. at onboarding or after a material change in the business relationship or following a review during ongoing CDD and account monitoring) or if it becomes apparent, after having established a business relationship with a Merchant, that one or more Merchant applications were approved but CDD (including, where applicable, Delayed Verification or EDD) was incorrectly conducted at onboarding or any other stage (i.e. Venue Smart does not have the appropriate KYC or screening data on file) then the following steps need to be undertaken:

- the Compliance Manager should be notified immediately;

- the relevant Merchant's ability to process transaction through the PayFac/Aggregation service must immediately cease until the issue is rectified or, if the issue cannot be rectified, then the business relationship with the Merchant must be terminated;
- A **full audit** on all applications processed since the last audit should be undertaken;
- The appropriate Payments Operations Team members responsible are to be retrained and where appropriate counseled;
- All incomplete applications are to be brought up to standard by obtaining the correct data/documentation and where necessary contacting the Merchant for the additional data;
- the Compliance Manager must consider (irrespective of whether the business relationship is terminated or not) whether to submit a suspicious activity report.

13. Suspicious activity reports

If a Merchant enquires about, conducts, or seeks to conduct, a transaction through Venue Smart or the PayFac/Aggregation service and Venue Smart / the Payments Operations Team has reasonable grounds to suspect that the transaction, or proposed transaction, is, or may be, related to criminal activity such as money laundering or terrorist financing including any transaction or proposed transaction that is or may be:

- Relevant to the investigation or prosecution of any person for a money laundering offence;
- Relevant to the enforcement of the Terrorism Suppression;
- Relevant to the enforcement of the Criminal Proceeds Recovery,

Then the Payment Operations Team must escalate the suspicion to the Compliance Manager and undertake EDD of the relevant Merchant. The Payments Operations Team must ensure that in conducting the EDD it does not tip-off the Merchant that a suspicious activity report will, or may, be submitted. Unlawful disclosure of suspicious activity reports (and Prescribed Transaction reports) is an offence.

The Payments Operations Team may also form a suspicion of money laundering or terrorist financing from, for example:

- A Merchant's reluctance to provide the required CDD information;
- A Merchant's provision of false CDD information; or
- Activities discovered in Venue Smart's account monitoring or ongoing CDD process.

After conducting EDD, the Compliance Manager must make a determination (based on information that would objectively justify a suspicion) whether there are reasonable grounds to suspect that the transaction, or proposed transaction, is, or may be, related to criminal activity such as money laundering or terrorist financing and, if applicable, submit a suspicious activity report to the Card Acquirer, Service Provider or Austrac no later than three working days after forming that suspicion. Only the Compliance Manager is permitted to submit suspicious activity reports. The Compliance Manager must write up and keep a record of any decisions it makes in relation to submitting, or choosing not to submit, a suspicious activity report.

The Compliance manager must keep a copy of any suspicious activity report that it submits (including any related resubmitted suspicious activity report and all relevant underlying information that supports the suspicion) for a period of at least 7 years after the report is made.

Urgent suspicious activity reports can be made orally by the Compliance Manager but the Compliance Manager must, as soon as practicable, and within three working days, forward the suspicious activity report to the Card Acquirer, Service Provider or Austrac.

14. Prescribed Transaction Reports

If a Merchant conducts a Prescribed Transaction through Venue Smart or the PayFac/Aggregation service, the Compliance Manager must submit a Prescribed Transaction report (in the prescribed form) to the Card Acquirer or Service Provider within 10 working days of the transaction which contains the following information:

- A description of the nature of the transaction;
- The amount of the transaction and the currency in which it was denominated;
- The date on which the transaction was conducted;
- The parties to the transaction;
- If applicable, the name of the facility (i.e. account or arrangement provided by Venue Smart) through which the transaction was conducted, and any other facilities (whether or not provided by Venue Smart) directly involved in the transaction; and
- Any other information prescribed by regulations.

Note: Prescribed Transaction reports for international wire transfers must be submitted by the:

- "Ordering institution" (i.e. any person who has been instructed by a person (the **payer**) to electronically transfer funds controlled by the payer to a person (the **payee**) who may or may not be the payer on the basis that the transferred funds will be made available to the payee by a "beneficiary institution"; and (b) includes a person declared by regulations to be an "ordering institution" for the purposes of the AML/CFT Act; but (c)

excludes a person or class of persons declared by regulations not to be an "ordering institution" for the purposes of the AML/CFT Act); or

- "Beneficiary institution" (i.e. any person who receives wire transfer funds and then makes those funds available to a person (the **payee**) by (a) crediting it to an account held by the payee; or (b) paying it to the payee,

accordingly, before submitting a Prescribed Transaction report for international wire transfers the Compliance Manager must be satisfied that Venue Smart is either the ordering or beneficiary institution.

15. Deviations from or non-compliance with the AML/CFT Policy

The aim of this policy is not to be commercially restrictive but more to reduce the risk profile of the business by ensuring Venue Smart is comfortable that it knows who their customer is and as such is legally compliant.

Any KYC deviations from the listed policy by the Payments Operations Team are required to be approved in writing by the Compliance Manager.

Venue Smart staff may face disciplinary action, which may lead to dismissal, if they fail to follow the procedures recorded in this AML/CFT Policy.

16. Customer review

All Merchants are to have their KYC data re-validated against the sanctions and PEP lists every 12 months.